FOURIER ANALYSIS ON FINITE GROUPS

A Thesis

by

JOSE MANUEL RIVERA MONTES DE OCA

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Chair of Committee,	Matthew Young
Committee Members,	Matthew Papanikolas
	Riad Masri
	Alan Dabney
Head of Department,	Emil Straube

August 2017

Major Subject: Mathematics

ABSTRACT

We start with some Fourier analysis on cyclic groups as the base case. This theory comes along with some basic notions about character theory. So, we develop some properties of the additive characters of $\mathbb{Z}/q\mathbb{Z}$. Formulas like the matrix version of the DFT, its inverse formula and Plancherel's theorem are proved for this case. Then, we give a constructive generalization to any finite abelian group. We also present some work on properties of characters in $\mathbb{Z}/q\mathbb{Z}^*$. All these tools are used to define and develop multiplicative characters. In particular, we mention Dirichlet characters and Gauss and Jacobi sums. The most important result of this work is to note that Fourier transform in $\mathbb{Z}/q\mathbb{Z}$ gives us a method to write a Dirichlet character in terms of additive characters. Finally, we apply some of this theory to Cayley graphs.

DEDICATION

A mi familia, por haberles tocado el trabajo más difícil.

To my family, for they did the real hard work.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supported by a thesis committee consisting of Professor Mathew Young [advisor], Professor Mathew Papanikolas and Professor Riad Masri of the Department of Mathematics and Professor Alan Dabney of the Department of Statistics.

All work for the thesis was completed by the student, under the advisement of Professor Mathew Young of the Department of Mathematics.

Funding Sources

There are no outside funding contributions to acknowledge related to the research and compilation of this document.

NOMENCLATURE

G	Finite abelian group
$L^2(G)$	Space of complex functions on G
$\mathbb{Z}/q\mathbb{Z}$	Cyclic group of order q
$\mathbb{T}$	Circle group (unit complex numbers)
$e(x)$	$e^{2\pi i x}$
$e_q(x)$	$e\left(\frac{x}{q}\right)$
$\psi_a(x)$	$e_q(ax)$
DFT	Discrete Fourier transform
$\mathcal{F}$	The DFT
$\widehat{f}$	DFT of f
F_q	DFT Matrix of size q
$x \sim y$	x adjacent to y
A_X	Adjacency matrix of the graph $X(\mathbb{Z}/q\mathbb{Z}, S)$
(a, b)	Greatest common divisor of a and b
$[a, b]$	Least common multiple of a and b
$\mathbb{Z}/q\mathbb{Z}^*$	Multiplicative group of $\mathbb{Z}/q\mathbb{Z}$
$G_\chi(a)$	Gauss sum of χ and ψ_a

TABLE OF CONTENTS

Page

1. INTRODUCTION

The Fourier transform was first defined by Joseph Fourier in 1822. Since then, it has been widely studied and the concept has expanded to several areas within Mathematics. As one of these generalizations, many scientists have been producing results concerning the discrete case, which is commonly known as the Discrete Fourier transform (DFT). This is still a broad concept and there exist multiple approaches one can follow to study it. Moreover, there are still open problems that deal with this tool. We could mention, for example, that the computation speed problem brought forth The Fast Fourier transform algorithm, which is listed in the Top 10 Algorithms of 20th Century by the IEEE journal Computing in Science & Engineering[1]. This problem is still a work area not just for mathematicians but for a diverse group of scientists.

Along this work, we will be dealing with a very special type of Fourier analysis. The most basic case of our study begins with the Fourier transform over cyclic groups. As the reader may suspect, we follow this approach using the fact that every finite cyclic group is isomorphic to $\mathbb{Z}/q\mathbb{Z}$ for some integer q. The foremost benefit of this approach is that we will be able to use all the rules about modular arithmetic. Moreover, it will be fairly easy to extend some of these results to every integer number by using periodicity. Therefore, it is highly recommended that reader is well-familiarized with the structure of $\mathbb{Z}/q\mathbb{Z}$.

As we will see in the following pages, there are two main structures we will be working with. The first are groups, as we have already stated, and the second one are, of course, the complex numbers. If we were to put this analysis in a production line, the input of the theory will be a finite abelian group. Then, we will construct some theory using the relations between this group and the complex numbers and, finally, Fourier analysis will

[1] J. Dongarra and F. Sullivan, *Guest Editors Introduction to the top 10 algorithms*. Computing in Science Engineering, January 2010.

give us some specific properties that we can use for that particular group. Actually, in the next chapter we introduce the basic elements over which the whole theory will work. Those are functions from the given group to the complex numbers.

Many of the results that we mention in this work could be found in any book about some variety of different subjects. However, our goal is aimed to be useful in number theoretic environments. So, as reader may suspect, the final objective of our work is giving the basics of some of the ideas of character theory that are used in multiplicative number theory. Therefore, we can say that the main result of this work is to define Dirichlet characters and look at their relation with Fourier transform as functions from a certain group into the complex numbers.

2. FOURIER ANALYSIS ON CYCLIC GROUPS

2.1 Space of functions

Fix $q \in \mathbb{Z}$, $q > 1$. We will start with the definition and some properties of the Fourier transform for the finite abelian group $\mathbb{Z}/q\mathbb{Z}$. Such analysis requires a quick review of the space of complex-valued functions on $\mathbb{Z}/q\mathbb{Z}$, which will be denoted as:

$$L^2(\mathbb{Z}/q\mathbb{Z}) = \{f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}\}.$$

Moreover, we look at $L^2(\mathbb{Z}/q\mathbb{Z})$ as a $\mathbb{C}$-vector space. In this case, its dimension will be q, but we will see that for a general abelian group G, the $\mathbb{C}$-vector space $L^2(G)$ has also finite dimension, $|G|$, and we can easily find a basis.

Proposition 2.1. *The $\mathbb{C}$-vector space $L^2(\mathbb{Z}/q\mathbb{Z})$ has dimension q. Moreover,*

$$L^2(\mathbb{Z}/q\mathbb{Z}) = \textit{span}\{\delta_i\}_{i\in\mathbb{Z}/q\mathbb{Z}},$$

with $\delta_i : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ defined by

$$\delta_{i=x} = \delta_i(x) = \begin{cases} 1 & \textit{if } x = i, \\ 0, & \textit{otherwise.} \end{cases}$$

We will refer to $\{\delta_i\}_{i\in\mathbb{Z}/q\mathbb{Z}}$ as the canonical basis for $L^2(\mathbb{Z}/q\mathbb{Z})$. This space can be equipped with an inner product $\langle f, g\rangle := \sum_{a\in\mathbb{Z}/q\mathbb{Z}} f(a)\overline{g(a)}$ for $f, g \in L^2(\mathbb{Z}/q\mathbb{Z})$. It can be easily verified that $\langle\cdot,\cdot\rangle$ is indeed an inner product, and as such, we will be using its linearity further along. As we will see in future chapters, our analysis will persistently need the notion of orthogonality between two given functions. So, given functions $f, g \in$

$L^2(\mathbb{Z}/q\mathbb{Z})$, they are called **orthogonal** whenever $\langle f, g\rangle = 0$. Now, consider the following definition.

Definition 2.2. *For $f, g \in L^2(\mathbb{Z}/q\mathbb{Z})$, the **convolution of** f **with** g is defined as*

$$(f * g)(x) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} f(y)\, g(x-y).$$

The operation $*$ gives $L^2(\mathbb{Z}/q\mathbb{Z})$ the structure of an abelian semigroup. That is, $f * g \in L^2(\mathbb{Z}/q\mathbb{Z})$, $f * (g * h) = (f * g) * h$ and $f * g = g * f$. The following are two notable cases:

i. $\delta_x * \delta_y = \delta_{x+y \pmod q}$.

ii. $f * \delta_y(x) = f(x-y)$.

2.2 Additive characters and orthogonality

Hereafter, we will write $e(x) := e^{2\pi i x}$ and $e_q(x) := e\left(\frac{x}{q}\right)$. We start this section with the following general definition.

Definition 2.3. *Let G be a finite abelian group written additively. A function $\psi\colon G \to \mathbb{C}^*$ such that $\psi(x+y) = \psi(x)\psi(y)$ for every $x, y \in G$ is called **a character of** G. If $\psi(x) = 1$ for all $x \in G$, then ψ is called the **trivial character**.*

Notice that, in the case $\mathbb{Z}/q\mathbb{Z}$, the function defined by $\psi_a(x) = e_q(ax)$ is a character of $\mathbb{Z}/q\mathbb{Z}$ for any given $a \in \mathbb{Z}/q\mathbb{Z}$. See that it is a group homomorphism between $\mathbb{Z}/q\mathbb{Z}$ and $\mathbb{T}$, the circle group. Moreover, $\mathbb{Z}/q\mathbb{Z}$ being cyclic means that we only need to know $\psi_a(1)$ to define ψ_a completely. Also see that $\psi_a(1)$ must be a q-th root of unity, thus there are exactly q possibilities for it. Since we can do this for each $a \in \mathbb{Z}/q\mathbb{Z}$, we have that the set $\{\psi_a\}_{a \in \mathbb{Z}/q\mathbb{Z}}$ has all the characters of $\mathbb{Z}/q\mathbb{Z}$. We will often call these functions the additive characters of $\mathbb{Z}/q\mathbb{Z}$. In this case, ψ_0 is the trivial character.

Lemma 2.4. *Given $a \in \mathbb{Z}/q\mathbb{Z}$, then*

$$\langle \psi_a, \psi_0 \rangle = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \psi_a(y) = q\delta_{a=0}.$$

Proof. Let $S := \langle \psi_a, \psi_0 \rangle$. First suppose that $a \equiv 0 \pmod{q}$, then $S = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} 1 = q$. Now suppose otherwise ($a \not\equiv 0 \pmod{q}$), then

$$\psi_a(1) S = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \psi_a(1) \psi_a(y) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \psi_a(y+1) = \sum_{z \in \mathbb{Z}/q\mathbb{Z}} \psi_a(z) = S.$$

Notice we are using that, for $z = y + 1$, if y runs through $\mathbb{Z}/q\mathbb{Z}$, then z also does. Finally see that $\psi_a(1) S = S$ implies that $S = 0$, since $\psi_a(1) \neq 1$ for $a \not\equiv 0 \pmod{q}$. This completes the proof. □

Theorem 2.5. *Given $a, b \in \mathbb{Z}/q\mathbb{Z}$, then*

$$\langle \psi_a, \psi_b \rangle = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \psi_a(y) \psi_b(-y) = q\delta_{a=b}.$$

Proof. Using the previous lemma we just need to see that

$$\langle \psi_a, \psi_b \rangle = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \psi_a(y) \psi_b(-y) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \psi_{a-b}(y) = \langle \psi_{a-b}, \psi_0 \rangle = q\delta_{a=b}. \qquad \square$$

What Theorem 2.5 says is that any two different characters of $\mathbb{Z}/q\mathbb{Z}$ are orthogonal. Moreover, the inner product of congruent characters (characters coming from congruent elements) always equals q. Of course we can always find q non-pair-wise-congruent numbers in $\mathbb{Z}/q\mathbb{Z}$, so the set $\{\psi_a\}_{a \in \mathbb{Z}/q\mathbb{Z}}$ is an orthogonal basis for $L^2(\mathbb{Z}/q\mathbb{Z})$. We will refer to Theorem 2.5 as an orthogonality relation for the characters of $\mathbb{Z}/q\mathbb{Z}$.

Lemma 2.6. *Given $x \in \mathbb{Z}/q\mathbb{Z}$, then*

$$\sum_{a \in \mathbb{Z}/q\mathbb{Z}} \psi_a(x) = q\delta_{x=0}.$$

Proof. We just need to note the symmetry of the additive characters, that is $\psi_a(x) = \psi_x(a)$. Thus, we can use Lemma 2.4 and write

$$\sum_{a \in \mathbb{Z}/q\mathbb{Z}} \psi_a(x) = \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \psi_x(a) = q\delta_{x=0}. \qquad \square$$

Theorem 2.7. *Given $x, y \in \mathbb{Z}/q\mathbb{Z}$, then,*

$$\sum_{a \in \mathbb{Z}/q\mathbb{Z}} \psi_a(x)\,\overline{\psi_a(y)} = q\delta_{x=y}.$$

Proof. Again, we just need the lemma and so

$$\sum_{a \in \mathbb{Z}/q\mathbb{Z}} \psi_a(x)\,\psi_a(-y) = \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \psi_a(x-y) = q\delta_{x=y}. \qquad \square$$

We will refer to Theorem 2.7 also as an orthogonality relation in the set of additive characters of $\mathbb{Z}/q\mathbb{Z}$. Also note that the trivial character appears several times in these equalities as a special case for orthogonality.

2.3 Fourier transform on $\mathbb{Z}/q\mathbb{Z}$

Definition 2.8. *The **Discrete Fourier transform (DFT)** on $\mathbb{Z}/q\mathbb{Z}$ is defined as*

$$\mathcal{F}\colon L^2(\mathbb{Z}/q\mathbb{Z}) \to L^2(\mathbb{Z}/q\mathbb{Z})$$
$$f \mapsto \widehat{f},$$

where

$$\widehat{f}\,(x) = \langle f, \psi_x \rangle = \sum_{a \in \mathbb{Z}/q\mathbb{Z}} f\,(a)\,\psi_x\,(-a).$$

One of the most important properties of the DFT is that it is a linear bijection on $L^2\,(\mathbb{Z}/q\mathbb{Z})$. Linearity is inherited by linearity of $\langle \cdot, \cdot \rangle$ on its first entry. Now we remain to prove that the DFT is a bijection.

Theorem 2.9. *The DFT is a bijection.*

Proof. Let $\mathcal{G}\colon\ L^2\,(\mathbb{Z}/q\mathbb{Z}) \to L^2\,(\mathbb{Z}/q\mathbb{Z})$ given by

$$\mathcal{G}\,(f\,(x)) = \frac{1}{q}\hat{f}\,(-x) = \frac{1}{q}\,\langle f, \psi_{-x} \rangle\,. \tag{2.1}$$

Then, for an arbitrary $f \in L^2\,(\mathbb{Z}/q\mathbb{Z})$ we have that

$$\begin{aligned}\mathcal{G} \circ \mathcal{F}\,(f\,(x)) &= \mathcal{G}\,(\langle f, \psi_x \rangle) = \frac{1}{q}\,\langle \langle f, \psi_x \rangle\,, \psi_{-x} \rangle = \frac{1}{q} \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \left(\sum_{z \in \mathbb{Z}/q\mathbb{Z}} f\,(z)\,\psi_{-y}\,(z) \right) \psi_x\,(y) \\ &= \frac{1}{q} \sum_{z \in \mathbb{Z}/q\mathbb{Z}} f\,(z) \left(\sum_{y \in \mathbb{Z}/q\mathbb{Z}} \psi_y\,(x - z) \right) \psi_x\,(y) = \frac{1}{q} \sum_{z \in \mathbb{Z}/q\mathbb{Z}} f\,(z)\,q\delta_{x=z} = f\,(x)\,.\end{aligned}$$

Thus, $\mathcal{F}$ is a linear transformation over a finite dimensional vector space with a left inverse. Therefore, it is a bijection. □

See that now we have these two transformations from $L^2\,(\mathbb{Z}/q\mathbb{Z})$ to itself:

$$\widehat{f}\,(x) = \langle f, \psi_x \rangle = \sum_{a \in \mathbb{Z}/q\mathbb{Z}} f\,(a)\,\psi_x\,(-a), \tag{2.2}$$

and

$$f\,(x) = \frac{1}{q}\hat{\widehat{f}}\,(-x) = \frac{1}{q}\left\langle \widehat{f}, \psi_{-x} \right\rangle = \frac{1}{q} \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \widehat{f}\,(a)\,\psi\,(a). \tag{2.3}$$

We have that (2.2) allows us to transform any element of $L^2(\mathbb{Z}/q\mathbb{Z})$ and (2.3) gives us a way to recover the original function.

Now, recall from Proposition 2.1 that, for a function $f \in L^2(\mathbb{Z}/q\mathbb{Z})$, we can write $f = f_i\delta_i$. So it will be helpful to identify f with the vector $(f_i := f(i))_{0\le i\le q-1}$.

Proposition 2.10. *The Fourier transform matrix is given by*

$$F_q := (\psi_{j-1}(1-k))_{1\le j,k\le q}.$$

That is, for a given function $f \in L^2(\mathbb{Z}/q\mathbb{Z})$, we have

$$\widehat{f} = F_q \cdot f. \tag{2.4}$$

Proof. We have that

$$(\psi_{j-1}(1-k))_{1\le j,k\le q}(f_i)_{1\le i\le q} = \left(\sum_{i=1}^{q} f_{i-1}\psi_n(1-i)\right)_{1\le n\le q}.$$

So,

$$\begin{aligned}\sum_{n=0}^{q-1}\delta_n(x)\sum_{i=1}^{q} f_{i-1}\psi_n(1-i) &= \sum_{n=0}^{q-1}\sum_{i=1}^{q}\delta_n(x)\,f(i-1)\,\psi_n(1-i)\\ &= \sum_{i=1}^{q} f(i-1)\,\psi_x(1-i) = \sum_{y\in\mathbb{Z}/q\mathbb{Z}} f(y)\,\psi_x(-y) = \langle f,\psi_x\rangle.\end{aligned}$$

□

We can use the DFT matrix version to give another proof of Theorem 2.9. See that the DFT matrix, F_q, is a Vandermonde matrix (see [1]) with all different entries in its second column. Thus,

$$\det(F_q) = \prod_{0\le i<j\le q-1}(\psi_j(-1) - \psi_i(-1)) \neq 0. \tag{2.5}$$

Therefore, F_q is invertible. Thus, $\mathcal{F}$ is an 1-1 and onto linear transform on $L^2(\mathbb{Z}/q\mathbb{Z})$. We end this section with the following well-known properties of the DFT.

Theorem 2.11. *Given $f, g \in L^2(\mathbb{Z}/q\mathbb{Z})$,*

$$\widehat{f * g} = \widehat{f} \cdot \widehat{g}. \tag{2.6}$$

Proof.

$$\begin{aligned}
\widehat{f * g}(x) &= \langle f * g, \psi_x \rangle = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} (f * g)(y)\, \psi_x(-y) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \sum_{z \in \mathbb{Z}/q\mathbb{Z}} f(z)\, g(y-z) \psi_x(-y) \\
&= \sum_{w \in \mathbb{Z}/q\mathbb{Z}} \sum_{z \in \mathbb{Z}/q\mathbb{Z}} f(z)\, g(w)\, \psi(-z-w) \qquad \text{for } w = y - z \\
&= \left(\sum_{z \in \mathbb{Z}/q\mathbb{Z}} f(z)\, \psi_x(-z) \right) \left(\sum_{w \in \mathbb{Z}/q\mathbb{Z}} g(w)\, \psi_x(-w) \right) = \widehat{f} \cdot \widehat{g}.
\end{aligned}$$

□

Theorem 2.12 (Parseval's equality)**.** *Given $f, g \in L^2(\mathbb{Z}/q\mathbb{Z})$,*

$$\langle f, g \rangle = \frac{1}{q} \left\langle \widehat{f}, \widehat{g} \right\rangle \tag{2.7}$$

Proof. Using (2.3) we have that

$$\begin{aligned}
\langle f, g \rangle &= \sum_{y \in \mathbb{Z}/qZ} f(y) \overline{g(y)} = \sum_{y \in \mathbb{Z}/qZ} f(y) \overline{\frac{1}{q} \langle \widehat{g}, \psi_y \rangle} = \frac{1}{q} \sum_{y \in \mathbb{Z}/qZ} f(y) \sum_{z \in \mathbb{Z}/qZ} \overline{\widehat{g}(z)\, \psi_y(z)} \\
&= \frac{1}{q} \sum_{z \in \mathbb{Z}/qZ} \overline{\widehat{g}(z)} \sum_{y \in \mathbb{Z}/qZ} f(y)\, \psi_z(-y) = \frac{1}{q} \sum_{z \in \mathbb{Z}/qZ} \overline{\widehat{g}(z)} \widehat{f}(z) = \frac{1}{q} \left\langle \widehat{f}, \widehat{g} \right\rangle.
\end{aligned}$$

□

Corollary 2.13. *For* $f \in L^2(\mathbb{Z}/q\mathbb{Z})$,

$$\langle f, f \rangle = \frac{1}{q} \left\langle \widehat{f}, \widehat{f} \right\rangle. \tag{2.8}$$

3. THE GENERAL CASE

3.1 Character group of finite abelian groups

We have been solely working with $\mathbb{Z}/q\mathbb{Z}$ so far. Nonetheless, it is not hard to see that we can extend these results to any finite abelian group G[1]. We would just need to make some notational adjustments and consider the following theorem.

Theorem 3.1 (Structure theorem of finite abelian groups)**.** *For any finite abelian group G we can find $q_1, \dots q_n \in \mathbb{Z}$ such that*

$$G \cong \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_n\mathbb{Z}.$$

The proof of Theorem 3.1 can be found in almost any book about abstract algebra like [2], [3] or even in [1]. This way, we can write an element of G as $(a_1, \dots, a_n)$ and the sum will be done component-wise. Moreover, we still can define $L^2(G)$ as the complex vector space of functions on G and it will still have the inner product defined by $\langle f, g\rangle := \sum_{a\in G} f(a)\,\overline{g(a)}$. Now, we previously stated that the set of characters for $\mathbb{Z}/q\mathbb{Z}$ is the set $\{\psi_a\}_{a\in\mathbb{Z}/q\mathbb{Z}}$. See that we can define a multiplication in this set as $(\psi_a\psi_b)(x) := \psi_a(x)\,\psi_b(x)$. It is easy to prove that the set of additive characters of $\mathbb{Z}/q\mathbb{Z}$ has a group structure with respect to the multiplication we just defined. This can be done in general for any finite abelian group G.

Definition 3.2. *The set of all characters of G, which we will call $\widehat{G}$, forms an abelian group under point wise multiplication. This group is called **the character group** of G and its identity element will be the **trivial character**, denoted χ_0, which will be the one sending every element of G to 1.*

[1] Hereafter, we will assume every group G is finite and abelian.

It is not hard to see that a group character is really a homomorphism between G and $\mathbb{T}$. This is because if $x \in G$ is such that it has order a, then $1 = \chi(0_G) = \chi(a \cdot x) = \chi(x)^a$, where 0_G is the identity element of G, and so $\chi(x)$ is an a-th root of unity. This implies that the inverse of $\chi \in \widehat{G}$ is $\overline{\chi}(x) := \overline{\chi(x)}$ since $\chi(x)\overline{\chi}(x) = |\chi(x)|^2 = 1$. The deduction we just did gives us even more information about the group of characters of $\mathbb{Z}/q\mathbb{Z}$ for which we already had a definition of characters (Definition 3.2 is nothing else but an extension of the old definition). The fact that $\mathbb{Z}/q\mathbb{Z}$ is cyclic allows us to do $\chi(k) = \chi(1)^k$ for each $k \in \mathbb{Z}/q\mathbb{Z}$. This tells us that we only need to know the value of $\chi(1)$ to define χ completely. Furthermore, since $\chi(1)$ must be a q-th root of unity then there are q possible options where to send it, which means that there are at most q characters of $\mathbb{Z}/q\mathbb{Z}$. Recall from last chapter that we had already a set of exactly q additive characters, namely $\{\psi_a\}_{a\in\mathbb{Z}/q\mathbb{Z}}$. Finally, this tells us that $\widehat{\mathbb{Z}/q\mathbb{Z}} = \{\psi_a\}_{a\in\mathbb{Z}/q\mathbb{Z}}$.

Proposition 3.3. *$\mathbb{Z}/q\mathbb{Z} \cong \widehat{\mathbb{Z}/q\mathbb{Z}}$ as groups.*

Proof. Consider the following:

$$\phi\colon \mathbb{Z}/q\mathbb{Z} \to \widehat{\mathbb{Z}/q\mathbb{Z}}$$
$$a \mapsto \psi_a.$$

By the analysis we just did and by definition of ψ_a, we have that ϕ is an isomorphism. □

Proposition 3.4. *If G_1 and G_2 are two finite abelian groups then*

$$\widehat{G_1 \oplus G_2} \cong \widehat{G_1} \oplus \widehat{G_2} \quad \text{as groups.}$$

Proof. There are two ways we can do this. The long way would be to consider $\chi_1 \in \widehat{G_1}$ and $\chi_2 \in \widehat{G_2}$, and so $(\chi_1, \chi_2) \in \widehat{G_1} \oplus \widehat{G}$. Thus, we can make $\phi(a,b) := (\chi_1, \chi_2)(a,b) =$

$\chi_1(a)\,\chi_2(b)$ so that

$$\tau\colon \widehat{G_1} \oplus \widehat{G_2} \to \widehat{G_1 \oplus G_2}$$
$$(\chi_1, \chi_2) \mapsto \phi$$

is a group homomorphism. Moreover, if $\psi \in \widehat{G_1 \oplus G_2}$ and so ϕ distributes over sums, then we can do $\psi(a,b) = \psi(a,e_2)\,\psi(e_1,b)$ where e_1 and e_2 are the identities in G_1 and G_2 respectively. So let $\chi_1(a) = \psi(a,e_2)\ \forall a \in G_1$ and $\chi_2(b) = \psi(a,e_2)\ \forall b \in G_2$. Clearly $\chi_1 \in \widehat{G_1}$ and $\chi_2 \in \widehat{G_2}$. Therefore,

$$\sigma\colon \widehat{G_1 \oplus G_2} \to \widehat{G_1} \oplus \widehat{G_2}$$
$$\psi \mapsto (\chi_1, \chi_2)$$

is a homomorphism so that τ and σ are clearly inverses to each other and so we are done. The second way is to look at G_1, G_2 and $\mathbb{T}$ as $\mathbb{Z}$-modules, $\widehat{G_1}$ as $\mathrm{Hom}(G_1, \mathbb{T})$ and $\widehat{G_2}$ as $\mathrm{Hom}(G_2, \mathbb{T})$. Then invoke a theorem (which can be found in [3]) saying that if $\{M_i\}_{i\in I}$ is a collection of finitely generated $\mathbb{Z}$-modules and M is another $\mathbb{Z}$-module, then

$$\bigoplus_{i\in I} \mathrm{Hom}(M_i, M) \cong \mathrm{Hom}\left(\bigoplus_{i\in I} M_i, M\right) \quad \text{as groups.}$$

In our case $M_i = G_i$ for $i = 1, 2$, $M = \mathbb{T}$ and so the proof follows. □

Theorem 3.5. *Every finite abelian group is self-dual, i.e.* $G \cong \widehat{G}$.

Proof. Using Theorem 3.1 and Propositions 3.3 and 3.4 we have that

$$G \cong \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_n\mathbb{Z} \cong \widehat{\mathbb{Z}/q_1\mathbb{Z}} \oplus \cdots \oplus \widehat{\mathbb{Z}/q_n\mathbb{Z}} \cong (\mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_n\mathbb{Z})^\wedge \cong \widehat{G}.$$

□

For a finite abelian group G, if we still consider G under $+$, we can say even more about $\widehat{G}$. Using Theorem 3.1 we can write $G \cong \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_n\mathbb{Z}$ and so, for $a = (a_1, \ldots a_n) \in G$ we can define $\chi_a(x) := \psi_{a_1}(x_1) \cdots \psi_{a_n}(x_n)$ for all $x = (x_1, \ldots, x_n) \in G$. This way we can characterize all characters of G in terms of each $a \in G$.

3.2 Fourier transform, the general case

We begin this section with some more notation. Just as we did with $\mathbb{Z}/q\mathbb{Z}$, we can let $L^2(F)$ be the $\mathbb{C}$-vector space of all complex valued functions on a finite abelian group G. Similarly, we can define the inner product $\langle f, g\rangle := \sum_{a\in G} f(a)\overline{g(a)}$ for $f, g \in L^2(G)$ and the convolution of such functions as $(f * g)(x) = \sum_{y\in G} f(y)\, g(x-y)$ for all $x \in G$.

Definition 3.6. *The **Discrete Fourier transform (DFT)** on G is defined as*

$$\mathcal{F}\colon L^2(G) \to L^2\left(\widehat{G}\right)$$
$$f \mapsto \widehat{f},$$

where

$$\widehat{f}(\chi) = \langle f, \chi\rangle = \sum_{a\in G} f(a)\overline{\chi(a)} \quad \textit{for all } \chi \in \widehat{G}.$$

The very first thing that we can notice is that in this new definition the DFT goes to $L^2\left(\widehat{G}\right)$ instead of $L^2(G)$ as it was for the case $\mathbb{Z}/q\mathbb{Z}$ (Definition 2.8). This may not seem consistent, but, according to Theorem 3.5 we can replace $\widehat{G}$ by G in Definition 3.6 and so both definitions would agree then. Also, the properties we proved in last chapter hold equally for this general case, furthermore, the proofs can be slightly changed to get a proof for the new statements.

Theorem 3.7. *Let $f, g \in L^2(G)$, then,*

(i) ***The DFT is a bijection.***

(ii) ***Fourier inversion formula.***

$$f(x) = \frac{1}{|G|} \sum_{\chi \in G} \widehat{f}(\chi)\, \chi(x). \tag{3.1}$$

(iii) ***Convolution.***

$$\widehat{f * g} = \widehat{f} \cdot \widehat{g}.$$

(iv) ***Parseval's equality.***

$$\langle f, g \rangle = \frac{1}{|G|} \left\langle \widehat{f}, \widehat{g} \right\rangle.$$

The inner product on the RHS is defined on $L^2\left(\widehat{G}\right)$ *just as one could expect:*

$$\left\langle \widehat{f}, \widehat{g} \right\rangle = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\, \overline{\widehat{g}(\chi)}.$$

The proof of Theorem 3.7 is a reproduction of the ones of Theorems 2.9, 2.11 and 2.12. A remaining issue that might not be clear enough is to see that, in this case, $\{\delta_a\}_{a \in G}$ is a basis for $L^2(G)$, where

$$\delta_{a=x} = \delta_a(x) = \begin{cases} 1 & \text{if } x = a, \\ 0, & \text{otherwise} \end{cases} \qquad \text{for all } x \in G.$$

The last thing to clarify is that the orthogonality relations of characters of $\mathbb{Z}/q\mathbb{Z}$ still hold for the characters of G. More on, the proof of Theorem 3.8 below can be taken from Lemma 2.4 and Theorem 2.5. However, Theorem 3.9 will need some adjustments.

Theorem 3.8. *Given* $\chi_1, \chi_2 \in \widehat{G}$*,*

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} |G| & \text{if } \chi_1 = \chi_2, \\ 0, & \text{otherwise.} \end{cases} \tag{3.2}$$

A particular case is when χ_2 *is the trivial character. Then, for any* $\chi \in \widehat{G}$ *we have*

$$\sum_{y \in G} \chi(y) = \begin{cases} |G| & \text{if } \chi = \chi_0, \\ 0, & \text{otherwise.} \end{cases} \tag{3.3}$$

Theorem 3.9. *Given* $a, b \in G$*, we have*

$$\sum_{\chi \in \widehat{G}} \chi(a) \overline{\chi}(b) = \left|\widehat{G}\right| \delta_{a=b}. \tag{3.4}$$

In particular, if $b = 0_G$ *(the identity of* G*), we have*

$$\sum_{\chi \in \widehat{G}} \chi(a) = \left|\widehat{G}\right| \delta_{a=0_G}. \tag{3.5}$$

Proof. To prove (3.4) we can follow the same methodology we have been working with. Let S be the sum on the LHS of (3.4). First suppose $a = b$, then

$$S = \sum_{\chi \in \widehat{G}} \chi\overline{\chi}(a) = \sum_{\chi \in \widehat{G}} \chi_0(a) = \left|\widehat{G}\right|. \tag{3.6}$$

Now, if $a \neq b$ we can find $\phi \in \widehat{G}$ such that $\phi(a - b) \neq 1$ (otherwise, every $\phi \in \widehat{G}$ would be trivial and we know there are $|G|$ of them). In particular see that

$$\phi(b)\overline{\phi}(b) = \phi\overline{\phi}(b) = \phi_0(b) = 1 = \phi(0_G) = \phi(b - b) = \phi(b)\phi(-b) \Rightarrow \overline{\phi}(b) = \phi(-b).$$

So, $\phi(a-b) = \phi(a)\,\phi(-b) = \phi(a)\,\overline{\phi}(b)$. Multiplying (3.6) by $\phi(a-b)$ we get

$$\phi(a-b)\,S = \sum_{\chi\in\widehat{G}} \phi(a)\,\overline{\phi}(b)\,\chi(a)\,\overline{\chi}(b) = \sum_{\chi\in\widehat{G}} \psi\chi(a)\,\overline{\psi\chi}(b) = \sum_{\varphi\in\widehat{G}} \varphi(a)\,\overline{\varphi}(b) = S.$$

In this last equality we are making $\varphi = \psi\chi$ and the sum over χ will run as fast as the sum over φ since $\widehat{G}$ is a group. Finally $\phi(a-b) \neq 1$ implies that $S = 0$. □

4. THE MULTIPLICATIVE CASE

In this chapter we will apply the Fourier analysis we did in Chapter 3 to the multiplicative group $\mathbb{Z}/q\mathbb{Z}^*$. Changing everything in Chapter 3 from additive to multiplicative notation will give us the theory we need. The upshot of this chapter is to find that the DFT serves as a bridge between what we will call multiplicative characters and the old additive characters.

4.1 Dirichlet characters

Let $\chi \in \widehat{\mathbb{Z}/q\mathbb{Z}^*}$, extend χ to $\mathbb{Z}/q\mathbb{Z}$ by defining $\chi(x) = 0$ for all x such that $(x, q) > 1$. Extend to all $\mathbb{Z}$ by periodicity. So we have

$$\chi(x) = \begin{cases} \chi([x]) & \text{if } (x,q) = 1, \\ 0, & \text{otherwise} \end{cases} \qquad \forall x \in \mathbb{Z}, \tag{4.1}$$

where $[x]$ is the class of x in $\mathbb{Z}/q\mathbb{Z}$. This way we have that χ is defined for all $\mathbb{Z}$, but preserves its values as a character of $\mathbb{Z}/q\mathbb{Z}^*$.

Definition 4.1. *A function $\chi\colon \mathbb{Z} \to \mathbb{C}$ holding* (4.1) *is called* ***a Dirichlet character modulo*** *q. The extension of the trivial character is called* ***the principal character****.*

The idea of this Dirichlet characters is to look at them as functions $\chi\colon \mathbb{Z} \to \mathbb{C}$ having three properties: it is multiplicative (i.e. $\chi(ab) = \chi(a)\chi(b) \forall a, b \in \mathbb{Z}$), it is zero at x if and only if x and q are not relatively prime (i.e. $\chi(x) = 0 \Leftrightarrow (x, q) > 0$), and it is periodic (i.e. exists q such that $\chi(a + q) = \chi(a)$). See that we still can let $\overline{\chi}(x) = \overline{\chi(x)}$ so that $\chi\overline{\chi}(a)$ will be 1 whenever $(a, q) = 1$ and 0 otherwise. Recall that the order of $\mathbb{Z}/q\mathbb{Z}^*$ is $\varphi(q)$, where φ is the Euler's totient function (see [4] for details). For any χ, χ_1, χ_2 Dirichlet characters modulo q and $a, b \in \mathbb{Z}/q\mathbb{Z}^*$, we can write the four orthogonality

relations as:

$$\sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi_1(y)\,\overline{\chi_2}(y) = \begin{cases} \varphi(q) & \text{if } \chi_1 = \chi_2, \\ 0, & \text{otherwise,} \end{cases} \tag{4.2}$$

$$\sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi(y) = \begin{cases} \varphi(q) & \text{if } \chi = \chi_0, \\ 0, & \text{otherwise,} \end{cases} \tag{4.3}$$

$$\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}^*}} \chi(a)\,\overline{\chi}(b) = \begin{cases} \varphi(q) & \text{if } (ab,q) = 1, \\ 0, & \text{otherwise,} \end{cases} \tag{4.4}$$

$$\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}^*}} \chi(a) = \begin{cases} \varphi(q) & \text{if } a = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{4.5}$$

See that in (4.2) and (4.3) the sums run though $\mathbb{Z}/q\mathbb{Z}$ rather than in $\mathbb{Z}/q\mathbb{Z}^*$. This is because, for any Dirichlet character modulo q, $\chi(y) = 0$ for all $y \in \mathbb{Z}/q\mathbb{Z}$ with $(y,q) > 1$. Now, the group $\widehat{\mathbb{Z}/q\mathbb{Z}^*}$ deals only with characters of the same modulus, q. Nonetheless, we can multiply characters of different moduli too.

Proposition 4.2. *Let χ_1,χ_2 be Dirichlet characters modulo q_1 and q_2 respectively, then $\chi_1\chi_2$ is a Dirichlet character modulo $[q_1, q_2]$.*

Proof. Let $m, n \in \mathbb{Z}$, then:

Multiplicativity.

$$\chi_1\chi_2(mn) = \chi_1(mn)\,\chi_2(mn) = \chi_1(m)\,\chi_2(m)\,\chi_1(n)\,\chi_2(n) = \chi_1\chi_2(m)\,\chi_1\chi_2(n).$$

Periodicity. We want to find $k \in \mathbb{Z}$ such that $\chi_1\chi_1(n+k) = \chi_1\chi_1(n)$ for all $n \in \mathbb{Z}$. The

claim is that $k = [q_1, q_2]$. So,

$$\chi_1\chi_2\left(n + [q_1, q_2]\right) = \chi_1\left(n + [q_1, q_2]\right)\chi_2\left(n + [q_1, q_2]\right) = \chi_1\left(n\right)\chi_2\left(n\right) = \chi_1\chi_2\left(n\right).$$

Zeros. We have that $d := (n, [q_1, q_2]) = 1$ if and only if $d \mid q_1$ and $d \mid q_2$. So, suppose first that $d > 1$. Then, without loss of generality, suppose $d \mid q_1$ and so $(n, q_1) > 1$. Thus,

$$\chi_1\chi_2\left(n\right) = \chi_1\left(n\right)\chi_2\left(n\right) = 0.$$

For $d = 1$, suppose $\chi_1\chi_2\left(n\right) = 0$, then, without loss of generality, suppose $\chi_1\left(n\right) = 0$). So $k\colon = (n, q_1) > 1$, and thus $k \mid n$ and $k \mid q_1$, but also $k \mid [q_1, q_2]$ and so $k > d$ which leads us to a contradiction. □

By Theorem 3.5, we know that there are exactly $\varphi\left(q\right)$ multiplicative characters of $\mathbb{Z}/q\mathbb{Z}^*$. Moreover, as we did for the characters of the additive group $\mathbb{Z}/q\mathbb{Z}$, see that the orthogonality relations tells us that $\widehat{\mathbb{Z}/q\mathbb{Z}^*}$ is a basis for $L^2\left(\mathbb{Z}/q\mathbb{Z}^*\right)$. Hence, we know two different basis for $L^2\left(\mathbb{Z}/q\mathbb{Z}^*\right)$: the canonical (delta functions) and the multiplicative. If we restrict additive characters to the multiplicative group, we get what are usually called *Ramanujan sums*. These sums are a particular case of a Gauss sum, which we will introduce in the next section. Several special cases of Ramanujan sums can be found in [5].

Definition 4.3. *Let χ a Dirichlet character mod q. Suppose $0 < d \leq q$ is a divisor of q. If $\chi\left(a\right) = 1$ whenever $a \equiv 1 \pmod{d}$ and $(a, q) = 1$, then we say that d is an **induced modulus** for χ.*

It is easy to see that 1 is always an induced modulus of χ_0. More on, this is the only case when this can happen, that is, 1 is an induced modulus for χ if and only if $\chi = \chi_0$. See also that definition includes $k = q$ and we always have that q is an induced modulus for a Dirichlet character mod q. This gives us the following definition.

Definition 4.4. *A Dirichlet character χ mod q is called primitive whenever its only induced modulus is q.*

For the case when q is prime we have that its only divisors are 1 and q itself. So, if $\chi \neq \chi_0$, then χ has no induced modulus other than q. Therefore, for q prime, every non-principal Dirichlet character χ mod q is primitive. Now, suppose χ is a Dirichlet character mod q and we can write it as $\chi = \chi_0\chi'$, where χ_0 is the principal character mod q and χ' is some Dirichlet character mod q' with $q' \mid q$, $q' \neq q$. See that Proposition 4.2 implies that χ is not principal and the converse implication is also true. So, a Dirichlet character χ mod q is primitive if and only if we can find a Dirichlet character χ' mod q' for some $q' \mid q$, $q' \neq q$, such that $\chi = \chi_0\chi'$.

4.2 Gauss sums

Definition 4.5. *For any finite commutative ring R with additive group R^+ and unit group R^*, let $\widehat{R^+}$ and $\widehat{R^*}$ be the additive and multiplicative character groups respectively. Let $\psi \in \widehat{R^+}$ and $\chi \in \widehat{R^*}$ extended to non-units where it takes the value 0, then,* ***the Gauss sum of χ and ψ is defined as***

$$G(\chi, \psi) := \left\langle \chi, \overline{\psi} \right\rangle = \sum_{r \in R} \chi(r)\, \psi(r).$$

In particular, for $R = \mathbb{Z}/q\mathbb{Z}$ we will use the notation

$$G_\chi(a) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \chi(y)\, \psi_a(y).$$

Gauss sums have been widely studied and more information about them can be found in [6], [5] or [7]. In this section we will limit ourselves to prove the following properties.

Lemma 4.6. *If χ is a Dirichlet character mod q and $a \in \mathbb{Z}/q\mathbb{Z}^*$, then*

$$G_\chi(a) = \bar{\chi}(a)\, G_\chi(1).$$

Proof.

$$\begin{aligned} G_\chi(a) &= \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \chi(y)\, \psi_a(y) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \chi(a)\, \bar{\chi}(a)\, \chi(y)\, \psi_a(y) \\ &= \bar{\chi}(a) \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \chi(ay)\, \psi_a(y) = \bar{\chi}(a) \sum_{m \in \mathbb{Z}/q\mathbb{Z}} \chi(m)\, \psi_1(m) = \bar{\chi}(a)\, G_\chi(1). \end{aligned}$$ □

Corollary 4.7. *The following are particular cases for $G_\chi(0)$:*

(i) $\chi \neq \chi_0 \Rightarrow G_\chi(0) = 0$.

(ii) $G_{\chi_0}(0) = \varphi(q)$.

Proof. (i) $G_\chi(0) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \chi(y)\, \psi_0(y) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \chi(y) = 0$.

(ii) $G_{\chi_0}(0) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \chi_0(y)\, \psi_0(y) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}^*} \psi_0(y) = \varphi(q)$. □

Proposition 4.8. *With the same hypothesis as in Lemma 4.6, $|G_\chi(a)|^2 = |G_\chi(1)|^2$.*

Proof. Since $|\bar{\chi}(a)| = 1$, using the lemma we get:

$$|G_\chi(a)|^2 = |\bar{\chi}(a)|^2\, |G_\chi(1)|^2 = |G_\chi(1)|^2.$$ □

Corollary 4.9. *For q prime and $\chi \neq \chi_0$, $|G_\chi(a)|^2 = q$.*

Proof. We have that

$$|G_\chi(a)|^2 = |G_\chi(1)|^2 = G_\chi(1)\, \overline{G_\chi(1)} = G_\chi(1) \sum_{m \in \mathbb{Z}/q\mathbb{Z}} \bar{\chi}(m)\, \psi_1(-m).$$

By hypothesis, $(m,q) = 1$ for all $m \neq 0$ and $\chi \neq \chi_0$, so we can use Lemma 4.6 and Corollary 4.7 to see that $G_\chi(1)\,\bar{\chi}(m) = G_\chi(m)$ for all $m \in \mathbb{Z}/q\mathbb{Z}$, so,

$$|G_\chi(a)|^2 = \sum_{m\in\mathbb{Z}/q\mathbb{Z}} G_\chi(m)\,\psi_1(-m) = \sum_{m\in\mathbb{Z}/q\mathbb{Z}}\sum_{n\in\mathbb{Z}/q\mathbb{Z}} \chi(n)\,\psi_m(n)\psi_1(-m)$$
$$= \sum_{n\in\mathbb{Z}/q\mathbb{Z}} \chi(n) \sum_{m\in\mathbb{Z}/q\mathbb{Z}} \psi_m(n-1) = \sum_{n\in\mathbb{Z}/q\mathbb{Z}} \chi(n)\,q\delta_{n=1} = q. \qquad \square$$

Theorem 4.10. *Let χ be a Dirichlet character mod q and suppose we are given $n \in \mathbb{Z}$ not relatively prime to q such that $G_\chi(n) \neq 0$. Then χ is not primitive.*

Proof. We need to find d such that $d \mid q$ and $d \neq q$ such that $\chi(a) = 1$ whenever $a \equiv 1 \pmod{d}$ and $(a,q) = 1$. We claim that $d = q/g$ with $g := (n,q) > 1$ is such induced modulus for χ. Let a be such that $a \equiv 1 \pmod{d}$ and $(a,q) = 1$. We just remain to prove that $\chi(a) = 1$. Thus,

$$G_\chi(n) = \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi(y)\,\psi_n(y) = \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi(ay)\,\psi_n(ay) = \chi(a) \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi(y)\,\psi_n(ay). \quad (4.6)$$

Now, make $a = 1 + dm$ for some $m \in \mathbb{Z}$ and $n = gk$ for some $k \in \mathbb{Z}$. See that

$$\psi_n(ay) = \psi_n(y + dmg) = \psi_n(y)\,\psi_n\left(\frac{mqy}{g}\right) = \psi_n(y)\,\psi_1(qmyk) = \psi_n(y).$$

Puting this last equation together with (4.6) we get

$$G_\chi(n) = \chi(a) \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi(y)\,\psi_n(y) = \chi(a)\,G_\chi(n).$$

By hypothesis $G_\chi(n) \neq 0$, so $\chi(a) = 1$ as we wanted. $\square$

Proposition 4.11. *If χ is a primitive Dirichlet character mod q, then:*

(i) $(a,q) > 1 \Rightarrow G_\chi(a) = 0$.

(ii) $G_\chi(a) = \bar{\chi}(a) G_\chi(1) \quad \forall a \in \mathbb{Z}$.

(iii) $|G_\chi(1)|^2 = q$.

Proof. For (i), suppose $G_\chi(a) \neq 0$. Using Theorem 4.10 we get a contradiction. Now, Lemma 4.6 gives us what we want for $(a, q) = 1$. The rest of the cases follow from (i). Finally, we can use the first two parts and Corollary 4.9 to get (iii). □

Definition 4.12. *Let χ_1 and χ_2 be both Dirichlet characters mod q. We define* ***the Jacobi sum of*** χ_1 ***and*** χ_2 *as*

$$\mathcal{J}(\chi_1, \chi_2) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}^*} \chi_1(y) \chi_2(1-y).$$

Theorem 4.13. *If χ, χ_1, χ_2 are Dirichlet characters mod q then,*

(i) $\mathcal{J}(\chi, \overline{\chi}) = -\chi(-1)$.

(ii) $\chi_1\chi_2$ *non-trivial* $\Rightarrow G_{\chi_1}(1) G_{\chi_2}(1) = \mathcal{J}(\chi_1, \chi_2) G_{\chi_1\chi_2}(1)$.

Proof. To prove (i) see that

$$\begin{aligned}\mathcal{J}(\chi, \overline{\chi}) &= \sum_{y \in \mathbb{Z}/q\mathbb{Z}^*} \chi(y) \overline{\chi}(1-y) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}^*} \overline{\chi}(y) \chi(1-y) \\ &= \sum_{y \in \mathbb{Z}/q\mathbb{Z}^*} \chi\left(y^{-1} - 1\right) = \sum_{y \in \mathbb{Z}/q\mathbb{Z}^*} \chi(y-1) = -\chi(-1).\end{aligned}$$

For (ii) consider the following.

$$\begin{aligned}G_{\chi_1}(1) G_{\chi_2}(1) &= \left(\sum_{y \in \mathbb{Z}/q\mathbb{Z}} \chi_1(y) \psi_1(y)\right) \left(\sum_{z \in \mathbb{Z}/q\mathbb{Z}} \chi_2(z) \psi_1(z)\right) \\ &= \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \sum_{z \in \mathbb{Z}/q\mathbb{Z}} \chi_1(y) \chi_2(z) \psi_1(y+z) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \psi_1(x) \sum_{y+z=x} \chi_1(y) \chi_2(z).\end{aligned} \tag{4.7}$$

Now, make $S(x) = \sum_{y+z=x} \chi_1(y)\chi_2(z)$ and see that for $x = 0$,

$$S(0) = \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi_1(y)\chi_2(-y) = \chi_2(-1)\sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi_1\chi_2(y) = 0.$$

This last step comes from an orthogonality relation and the fact that $\chi_1\chi_2 \neq \chi_0$. On the other hand, when $x \neq 0$ we can make

$$\begin{aligned}\sum_{x\neq 0} \psi_1(x) S(x) &= \sum_{x\neq 0} \psi_1(x) \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi_1(y)\chi_2(x-y) \\ &= \sum_{x\neq 0} \psi_1(x) \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \chi_1(xy)\chi_2(x-xy) = \mathcal{J}(\chi_1,\chi_2)\sum_{x\neq 0} \chi_1\chi_2(x)\psi_1(x) \\ &= \mathcal{J}(\chi_1,\chi_2) G_{\chi_1\chi_2}(1).\end{aligned}$$

Finally, we can write (4.7) as

$$G_{\chi_1}(1) G_{\chi_2}(1) = S(0) + \sum_{x\neq 0} \psi_1(x) S(x) = \mathcal{J}(\chi_1,\chi_2) G_{\chi_1\chi_2}(1). \qquad \square$$

4.3 Fourier transform on $(\mathbb{Z}/q\mathbb{Z})^*$

In this last section we consider the Fourier expansion of the Dirichlet characters. By the analysis we did in Chapter 3, we have that there are exactly $\varphi(q)$ Dirichlet characters mod q. So, even the isomorphism between $\mathbb{Z}/q\mathbb{Z}^*$ and $\widehat{\mathbb{Z}/q\mathbb{Z}^*}$ is not trivial, we can order them as $\chi_0, \ldots \chi_{\varphi(q)-1}$. Thus, for a Dirichlet character χ_n, its Fourier expansion is given by

$$\chi_n(x) = \sum_{y\in\mathbb{Z}/q\mathbb{Z}} c_\chi(y)\psi_x(y). \tag{4.8}$$

By the general inversion formula of the DFT (3.1), the coefficients $c_\chi(y)$ are given by

$$c_\chi(y) = \frac{1}{q} \sum_{z \in \mathbb{Z}/q\mathbb{Z}} \chi(z)\, \psi_{-y}(z) = \frac{1}{q} G_\chi(-y). \tag{4.9}$$

This way, the DFT gives us a way to write multiplicative characters in terms of additive characters. More on, we can look Dirichlet characters as elements of $L^2(\mathbb{Z}/q\mathbb{Z})$. So, what (4.9) is really giving us is an explicit formula for the coefficients of of Dirichlet characters as a linear combination of the additive basis. Finally, consider the following particular case.

Theorem 4.14. *The Fourier expansion of a primitive Dirichlet character χ has the form*

$$\chi(x) = \frac{\tau}{\sqrt{q}} G_{\overline{\chi}(-x)},$$

where

$$\tau = \frac{G_\chi(1)}{\sqrt{q}}.$$

Proof. By Proposition 4.11(ii), we can write $G_\chi(-y) = \bar{\chi}(-y)\, G_\chi(1)$. So, substituting in (4.8) we get that

$$c_\chi(y) = \frac{1}{q} \bar{\chi}(-y)\, G_\chi(1).$$

Finally, we can use (4.8) to get

$$\chi(x) = \frac{G_\chi(1)}{q} \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \bar{\chi}(-y)\, \psi_x(y) = \frac{G_\chi(1)}{q} \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \bar{\chi}(y)\, \psi_{-x}(y). \qquad \square$$

5. CAYLEY GRAPHS

In this chapter we will work with the basic theory of Cayley graphs. More information about graph theory can be found in [1] or [8]. Let $S \subset \mathbb{Z}/q\mathbb{Z}$ be a non-empty symmetric set. This means that if $s \in S$, then $-s \in S$. Consider the graph which vertices will be the elements of $\mathbb{Z}/q\mathbb{Z}$. For any two vertices x, y in the graph, they will be connected by an edge whenever exists $s \in S$ such that $x + s = y$. The fact that S is symmetric implies that if x is connected with y, then y is also connected with y. However, we will consider only undirected graphs. Thus, instead of drawing two directed edges, we will only draw a single undirected one. We will say that two vertices x and y are adjacent to each other when they are connected by an edge, and we will write it as $x \sim y$. Also, we could differentiate between edges coming from different elements of S by assigning a color to those generated by adding either s or $-s$. Still, we will not do this assignment and will consider only uncolored graphs. We will call these graphs $X(\mathbb{Z}/q\mathbb{Z}, S)$. See that if S is not a set of generators, then $X(\mathbb{Z}/q\mathbb{Z}, S)$ may not be connected, and if $0 \in S$, then we will have single loops at each vertex. Some notable choices for S are $S(r) := \{\pm r \pmod q\}$ or $B(r) := \{-r, -r+1, \ldots, r-1, r \pmod q\}$ for some $r \geq 1$. Examples of these graphs can be seen in Figure 5.1.

Definition 5.1. *For a graph $X(\mathbb{Z}/q\mathbb{Z}, S)$ with vertices $\{v_i\}_{0 \leq i \leq q-1}$, we define the **adjacency matrix**, A_X, as the $q \times q$ matrix whose i, j entry is 1 if $v_i \sim v_j$ and 0 otherwise.*

Recall from last chapter that for any $f \in L^2(\mathbb{Z}/q\mathbb{Z})$ we can find its coordinate vector with respect to the canonical basis. Now, see that for a graph $X(\mathbb{Z}/q\mathbb{Z}, S)$ with adjacency matrix A_X, we can let A_X act on f by multiplication. So, i-th entry of the vector $A_X \cdot f$ will have the sum of the values of f on x for all those $x \sim i$. So consider the following definition.

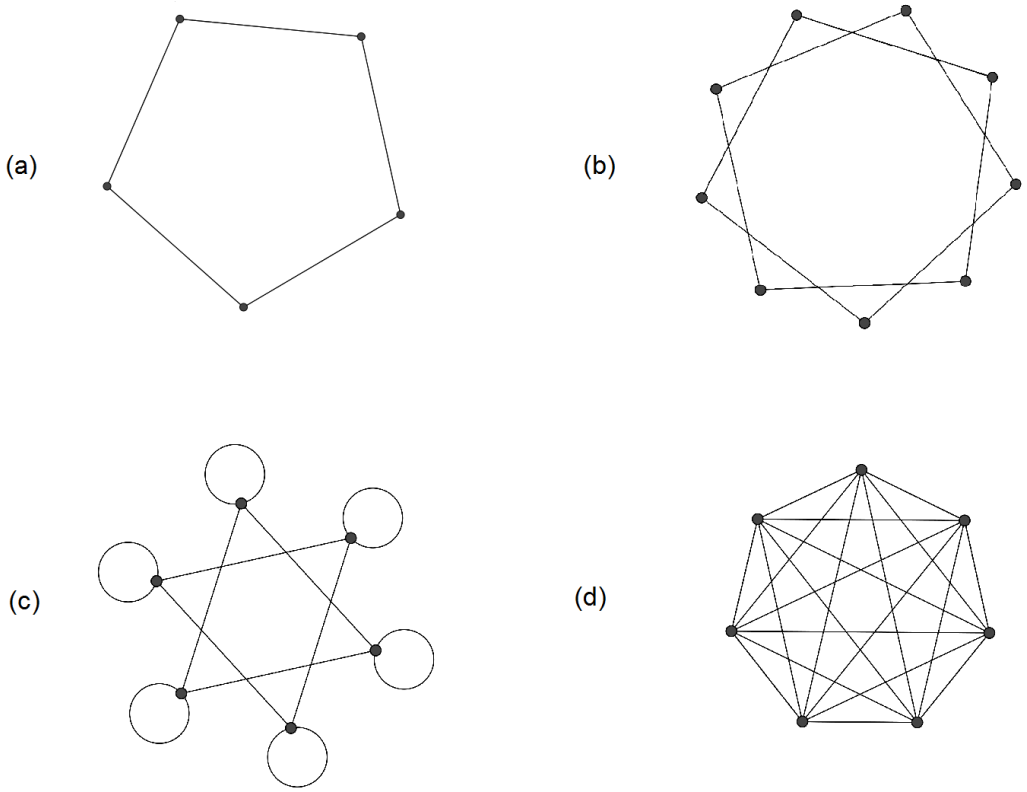

Figure 5.1: (a) $X(\mathbb{Z}/5\mathbb{Z}, S(1))$, (b) $X(\mathbb{Z}/9\mathbb{Z}, S(2))$, (c) $X(\mathbb{Z}/6\mathbb{Z}, S(2) \cup \{0\})$, (d) $X(\mathbb{Z}/7\mathbb{Z}, S(3) \setminus \{0\})$

Definition 5.2. *For a given graph $X(\mathbb{Z}/q\mathbb{Z}, S)$ with adjacency matrix A_X and $f \in L^2(\mathbb{Z}/q\mathbb{Z})$, let $A_X f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$, defined as*

$$A_X f(x) = \sum_{a \sim x} f(a).$$

For $S \subset \mathbb{Z}/q\mathbb{Z}$ the function $\delta_S(x)$ is 1 if $x \in S$ and 0 otherwise. So, we can write the action of the adjacency matrix on a function f as a convolution operator:

$$A_X f(x) = (\delta_S * f)(x). \tag{5.1}$$

Theorem 5.3. *The adjacency matrix A_X of a given graph $X(\mathbb{Z}/q\mathbb{Z}, S)$ is self-adjoint, that is, for all $f, g \in L^2(\mathbb{Z}/q\mathbb{Z})$ we have*

$$\langle A_X f, g\rangle = \langle f, A_X g\rangle .$$

Proof. By linearity of $\langle\cdot,\cdot\rangle$ we only need to show that $\langle A_X\delta_i, \delta_j\rangle = \langle\delta_i, A_X\delta_j\rangle$. So, on the LHS we have

$$\langle A_X\delta_i, \delta_j\rangle = \sum_{y\in\mathbb{Z}/q\mathbb{Z}} A_X\delta_i(y)\,\delta_j(y) = \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \delta_j(y)\sum_{a\sim y}\delta_i(a) = \sum_{a\sim j}\delta_{i=a} = \begin{cases} 1 & \text{if } j\sim i,\\ 0, & \text{otherwise}\end{cases}$$

while on the RHS we have

$$\langle\delta_i, A_X\delta_j\rangle = \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \delta_i(y)\,A_X\delta_j(y) = \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \delta_i(y)\sum_{a\sim y}\delta_j(a) = \sum_{a\sim i}\delta_{j=a} = \begin{cases} 1 & \text{if } i\sim j,\\ 0, & \text{otherwise.}\end{cases}$$

So the proof follows. □

So far, it seems like the Fourier analysis we did in last section has no influence in this graph-theoretic approach of finite groups. However, in Harmonic Analysis and spectral theory it is often useful to know the eigenvalues of an operator. Moreover, there are several classifications for Cayley graphs that rely on the eigenvalues of its adjacency matrix. This way, the following result becomes one of the most important applications of Fourier analysis to graph theory.

Theorem 5.4. *Consider the Cayley graph $X(\mathbb{Z}/q\mathbb{Z}, S)$. Then, the eigenvalues of its adjacency matrix are given by $\widehat{\delta_S}(a)$ for $a \in \mathbb{Z}/q\mathbb{Z}$.*

Proof. Take $f \in L^2(\mathbb{Z}/q\mathbb{Z})$. So, using (5.1) see that

$$\widehat{A_X f}(x) = \widehat{\delta_S * f}(x) = \widehat{\delta}_S(x)\,\widehat{f}(x).$$

Let $h = \widehat{f}$. Using (2.4) we can write this last equation in its matrix form as

$$\left(\left(F_q A_X F_q^{-1}\right) h\right)(x) = F_q \delta_S(x)\, h(x).$$

This means that when we apply $F_q A_X F_q^{-1}$ to a function h what we will get is a multiple of h, which means that $F_q A_X F_q^{-1}$ is diagonal. Moreover, the entries on its diagonal are $F_q \delta_S(x)$. So the eigenvalues of A_X will be $F_q \delta_S(a)$ for $a \in \mathbb{Z}/q\mathbb{Z}$. □

6. CONCLUSIONS AND FURTHER READING

After knowing the basic theory behind Dirichlet characters, it results almost natural to use DFT to build a relation between them and additive characters. In the beginning of this work, Terras' book ([1]) was the principal source of topics to be developed. The theory from chapters 2 and 3 follows the same methodology and contains similar results as in the book. However, none of the contents of chapter 4 can be found in it. More details about multiplicative number theory can be found in [9], [6], [7] and [10].

As an historical note, Dirichlet characters were first defined by Peter Gustav Lejeune Dirichlet in 1831. Back then, he was looking for functions from $\mathbb{Z}$ to $\mathbb{C}$ having the properties we stated in chapter 4. The most important use of Dirichlet characters is to define Dirichlet L-functions, which are common elements in books and papers about number theory nowadays. Thus, possible further readings may include topics in analytic number theory dealing with L-functions.

Furthermore, in chapter 5 we gave an application of DFT. Even though graph theory may seldom classify as pure mathematics, the number of industrial applications of it has been growing since its beginnings. This justifies the fact that there are more and more people doing research about it. In this work we presented very particular results that can be used to solve certain problems about graphs, but DFT has several other applications such as error correcting codes, compressing algorithms or even problems from physics and chemistry (some of them can be found in [1]).

All the theory developed in this work is sufficiently straightforward to be used either in analytic or algebraic number theory (doing a brief classification of topics in number theory). Nonetheless, the tools and ideas presented, DFT to be precise, are powerful enough that one can find them in much deeper notes or even research papers.

REFERENCES

[1] A. Terras, *Fourier Analysis on Finite Groups and Applications*. London Mathematical Society, Student Texts 43, 1999.

[2] T. Hungerford, *Algebra*. Springer, Graduate Texts in Mathematics 73, 2003.

[3] S. Lang, *Algebra*. Springer, Graduate Texts in Mathematics 211, 2005.

[4] G. A. Jones and J. M. Jones, *Elementary Number Theory*. Springer Undergraduate Mathematics Series, 2006.

[5] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*. Wiley-Interscience, 1998.

[6] T. M. Apostol, *Introduction to Analytic Number Theory*. Springer-Verlag, Undergraduate Texts in Mathematics, 1976.

[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. Springer-Verlag, Graduate Texts in Mathematics 84, 1990.

[8] M. Bona, *A Walk through Combinatorics: An Introduction to Enumeration and Graph Theory*. World Scientific Publishing Company, 2011.

[9] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*. Cambridge Studies in Advances Mathematics, 2007.

[10] H. Davenport, *Multiplicative Number Theory*. Springer-Verlag, Graduate Texts in Mathematics 74, 1980.